Bitcoin

Submitted By: Abhay Rana
Enrollment No: 09118001

Financial Management
MI-451

Introduction

Bitcoin is the world's first decentralized digital virtual currency. Currently, a single bitcoin is valued at over 23,000 INR. It is a software-based online payment system described by Satoshi Nakamoto in 2008, and released as open source software in 2009.

Being decentralized means that it is not regulated by any central bank, and that its production is not in the form of minting (as is the usual case with currencies), but rather bitcoins are created in a decentralized manner as a reward for transaction verification, as we will see later.

Is Bitcoin Money

An often raised question is the validity of Bitcoin's usage as money, given that it is not the official currency of any country on the planet. Neither has it been blessed by any major economy of the world.

To figure this out, we refer to the definition of money:

A commodity, asset or bill that may be exchanged for goods and services and serves some special requirements or functions:

1. Medium of exchange
2. Measure of value
3. Standard of deferred payment
4. Store of value

We note that none of these functions require the use of a central authority, and reach the conclusion that as long as there are people willing to transact in bitcoin, bitcoin can be considered as a unit of money.

Why Bitcoin?

Bitcoin offers the following four benefits over a normal currency:

1. **Decentralized:** Bitcoin is decentralized, meaning that it is not backed by any bank, and will hold its value nonetheless.

2. **Secure:** Bitcoin is cryptographically secure, and is guaranteed to be safe as long as certain common-sense precautions are taken. These precautions are basically keeping your private keys secure. As long as your private keys are safe, no one can seize your bitcoins.

3. **Anonymous:** Bitcoins being truly anonymous is actually a misnomer, as all transactions in bitcoin are stored in a public ledger. However, bitcoin is anonymous by virtue of the fact that you don't need to give any information about yourself to create a bitcoin address, through which you can send and receive bitcoins.

4. **Open Source:** Bitcoin being open source allows anyone in world (especially cryptographers) to understand and review the source code of Bitcoin, and help improve it. This means that any vulnerabilities in the bitcoin protocol are quickly found and patched. As Linus Torvalds once said: *"All bugs are shallow, given enough eyeballs".*

Who created Bitcoin?

Bitcoin was announced in 2008 in a research paper under the pseudonym of "Satoshi Nakamoto". This has since become quite famous, and yet it is still unknown who wrote that research paper.
Various guesses have been made by the media and researchers, but none have been conclusive so far.

How to get bitcoins?

Currently, 3 ways exist for an individual to get bitcoins:

1. via a Bitcoin exchange: Various bitcoin exchanges exist online that exchange a normal currency (such as USD) for bitcoins.
2. sell something for bitcoins: You can sell anything over the internet for bitcoins. Setting up a bitcoin address to receive bitcoins is a painless and free process. You can then sell something easily, in exchange for bitcoins.
3. mine bitcoins: New bitcoins are produced via a process called mining. Mining requires specialized hardware that must be bought and setup by you before you can get started with mining bitcoins.

Bitcoin Jargon

- ➔ *Bitcoin Address*: An identifier represents a possible destination for a Bitcoin payment.
- ➔ *Mining*: Mining is the process of adding transaction records to Bitcoin's public ledger of past transactions.
- ➔ *Blockchain*: A block chain is a transaction database shared by all nodes participating in a system based on the Bitcoin protocol
- ➔ *Transaction*: A transaction is a signed section of data that is broadcast to the network and collected into blocks.
- ➔ *P2P* (peer-to-peer): The Bitcoin network is peer to peer, meaning there is no need for a central server in the Bitcoin protocol.
- ➔ *Proof-of-work*: A proof of work is a piece of data which was difficult (costly, time-consuming) to produce so as to satisfy certain requirements. It must be trivial to check whether data satisfies said requirements.
- ➔ *Hash Function*: A hash algorithm turns an arbitrarily-large amount of data into a fixed-length hash.

How to create a Digital Currency?

Creating a digital currency is hard because of 2 problems:

1. Double Spending
2. Network based attacks

Double-spending is the result of successfully spending some money more than once. This would be the result if Bitcoin were naively implemented as a simple digital signature based currency. This would let a person spend the same coin twice.

Bitcoin protects against double spending by verifying each transaction added to the block chain to ensure that the inputs for the transaction had not previously already been spent.

Other electronic systems prevent double-spending by having a master authoritative source that follows business rules for authorizing each transaction. Bitcoin uses a decentralized system, where a consensus among nodes following the same protocol is substituted for a central authority.

Network-based attacks are possible when an attacker controls the majority of the nodes on the network. This is carefully handled in Bitcoin by making the voting system based on CPU power, instead of a simple majority of nodes in the network.

1 CPU = 1 Vote solves this issue by requiring the attacker to not just control the majority of the nodes, but also control majority of the processing power.

Proof of Work

A proof of work is a piece of data which was difficult (costly, time-consuming) to produce so as to satisfy certain requirements. It must be trivial to check whether data satisfies said requirements. Producing a proof of work can be a random process with low probability, so that a lot of trial and error is required on average before a valid proof of work is generated. Bitcoin uses the Hashcash proof of work.

For a block to be valid it must hash to a value less than the current target; this means that each block indicates that work has been done generating it. Each block contains the hash of the preceding block, thus each block has a chain of blocks that together contain a large amount of work. Changing a block (which can only be done by making a new block containing the same predecessor) requires regenerating all successors and redoing the work they contain. This protects the block chain from tampering.

The hard problem

Let's say the base string that we are going to do work on is "Hello, world!". Our target is to find a variation of it that SHA-256 hashes to a value beginning with '000'. We vary the string by adding an integer value to the end called a nonce and incrementing it each time. Finding a match for "Hello, world!" takes us 4251 tries (but happens to have zeroes in the first four digits):

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

Reward

Mining bitcoins is a computationally expensive process, thus requiring large amounts of electricity. (Comparable to a GPU). There are also costs associated with cooling hardware, which is usually used in tandem with mining hardware.

To entice people to become miners, Bitcoin rewards successful miners with bitcoins. This is the method by which new bitcoins are generated, and come into being.

When a block is discovered, the discoverer may award themselves a certain number of bitcoins, which is agreed-upon by everyone in the network. Currently this bounty is 25 bitcoins; this value will halve every 210,000 blocks, or around every 4 years.

Additionally, the miner is awarded the fees paid by users sending transactions. The fee is an incentive for the miner to include the transaction in their block. In the future, as the number of new bitcoins miners are allowed to create in each block dwindles, the fees will make up a much more important percentage of mining income.

The network is programmed to increase the money supply as a geometric series until the total number of Bitcoins reaches 21 million BTC. As of October 2012 slightly over 10 million of the total 21 million BTC had been created; the current total number created is available online. By 2013 half of the total supply will have been generated, and by 2017, three-quarters will have been generated. To ensure sufficient granularity of the money supply, clients can divide each BTC unit down to eight decimal places (a total of 2.1 × 1015 or 2.1 quadrillion units).

Whats next?

Bitcoin has often been labelled by many as a speculative bubble. This is true to some aspect, as there are still very few places where you can spend your bitcoins. Thus, currently the majority of Bitcoin’s value is only within itself, as a speculative currency.

In many ways, Bitcoin is similar to what the internet was in 1990s. It is still in its nascent days, and a lot of the world is still figuring out what can be possible with bitcoins. Bitcoin enthusiasts are divided on the opinion of bitcoin; one group says that bitcoin is overvalued, while the other hopes that it will continue to rise.

There is a need for more awareness about bitcoins and virtual currencies in general. Proper guidelines must be established around bitcoin security, similar to the PCI-DSS guidelines in the Payment Card Industry.

Bitcoin is, in many ways, the money of the future. It is digital, paperless, virtual, secure, and decentralized at the same time, making it an ideal choice for a currency.

Regardless of the direction bitcoin takes, it is a truly great solution to some really challenging problems in computer science and finances.